

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CN05/000133

International filing date: 31 January 2005 (31.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: CN
Number: 200410005740.0
Filing date: 16 February 2004 (16.02.2004)

Date of receipt at the International Bureau: 05 April 2005 (05.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

证 明

本证明之附件是向本局提交的下列专利申请副本

申 请 日： 2004.02.16

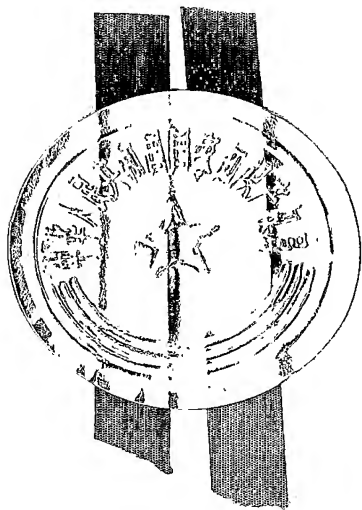
申 请 号： 2004100057400

申 请 类 别： 发明

发明创造名称： 密钥分发方法

申 请 人： 华为技术有限公司

发明人或设计人： 严军、吴东君



中华人民共和国
国家知识产权局局长

王 景 川

2005 年 2 月 18 日

权利要求书

1、一种密钥分发方法，应用于下一代网络中，所述下一代网络包括终端、软交换及认证中心，其特征在于，包括如下步骤：

- a) 终端向软交换发送注册请求消息；
- b) 软交换向认证中心发送认证请求消息；
- c) 认证中心对终端进行认证，同时生成所述终端与软交换的会话密钥，并在注册认证通过后，交由软交换向终端分发所述会话密钥。

2、根据权利要求 1 所述密钥分发方法，其特征在于，所述步骤 c) 具体包括：

c1) 认证中心根据与终端的共享密钥 Kc 生成对终端的第一验证字，同时生成所述终端与软交换之间的会话密钥，然后以所述共享密钥 Kc 对所述会话密钥加密，将加密后的会话密钥和第一验证字返回给软交换；

c2) 软交换向终端返回注册失败响应消息；

c3) 终端根据与认证中心的共享密钥 Kc 生成第二验证字，然后向软交换发送包含所述第二验证字的注册消息；

c4) 软交换根据认证中心提供的第一验证字与终端提供的第二验证字对所述终端进行认证，并在认证通过后，执行步骤 c5)；

c5) 软交换向终端返回注册成功响应消息，所述注册成功响应消息中包含经共享密钥 Kc 加密后的会话密钥，同时软交换向认证中心发出终端认证成功消息以便更新终端的相关信息；

c6) 终端根据所述共享密钥 Kc 解密认证中心加密过的会话密钥。

3、根据权利要求 2 所述密钥分发方法，其特征在于，步骤 c3) 所述注册消息还包含终端支持的安全能力列表及每种安全能力的优先级信息；

步骤 c4) 还包括软交换根据注册消息中终端的安全能力及每种安全能力的优先级信息选择一个合适的安全能力进行通信。

4、根据权利要求 2 所述密钥分发方法，其特征在于，所述下一代网络还包括信令代理，所述步骤 a) 具体包括：

终端向信令代理发送注册请求消息，信令代理向软交换转发终端的注册请求消息；

所述步骤 c1) 进一步包括:

认证中心获取与信令代理的共享密钥 K_{sp} , 然后以所述共享密钥 K_{sp} 对会话密钥进行加密, 并将经共享密钥 K_{sp} 加密后的会话密钥也返回给软交换;

所述步骤 c2) 具体包括:

软交换向信令代理返回注册失败响应消息, 信令代理向终端返回注册失败响应消息, 同时要求终端反馈支持的安全能力列表及每种安全能力的优先级信息;

所述步骤 c3) 具体包括:

终端将包含第二验证字、终端支持的安全能力列表以及每种安全能力的优先级信息的注册消息发送给信令代理, 信令代理根据终端支持的安全能力和每种安全能力的优先级信息选择一个合适的安全能力进行通信, 然后向软交换转发终端的注册消息;

所述步骤 c5) 具体包括:

软交换向信令代理转发终端注册成功响应消息, 所述注册成功响应消息中包含认证中心分别以共享密钥 K_c 和 K_{sp} 加密后的会话密钥, 信令代理用共享密钥 K_{sp} 解密认证中心经共享密钥 K_{sp} 加密过的会话密钥, 并以所述解密获取的会话密钥对注册成功响应消息报文计算报文验证字, 然后信令代理向终端转发注册成功响应消息, 所述注册成功响应消息中包含经共享密钥 K_{sp} 加密过的会话密钥、信令代理根据终端支持的安全能力选定的后续通信采用的安全能力项以及终端的安全能力参数列表和优先级信息以及所述报文验证字;

所述步骤 c6) 进一步包括:

终端利用解密后获取的会话密钥, 验证信令代理返回报文的报文验证字以验证信令代理身份, 同时验证报文的完整性以及信令代理返回的终端自己的安全能力参数是否正确, 并在验证通过后, 按照选定的安全能力进行通信。

5、根据权利要求 1-4 任一项所述密钥分发方法, 其特征在于, 所述注册请求消息和注册消息均为 SIP 协议注册消息, 所述注册失败响应消息为 SIP 协议响应消息, 所述注册成功响应消息为 SIP 协议注册请求成功消息。

6、根据权利要求 1-4 任一项所述密钥分发方法, 其特征在于, 所述注册请求消息为 MGCP 协议系统重启消息及其响应消息, 所述注册失败响应消息



和注册成功响应消息均为 MGCP 协议通知请求消息及其响应消息，所述注册消息为 MGCP 协议通知消息及其响应消息。

7、根据权利要求 1-4 任一项所述密钥分发方法，其特征在于，所述注册请求消息为 H.248 协议系统服务状态变化消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 H.248 协议属性更改消息及其响应消息，所述注册消息为 H.248 协议通知消息及其响应消息。

8、根据权利要求 1-4 任一项所述密钥分发方法，其特征在于，所述注册请求消息为 H.323 协议网守请求消息，所述注册失败响应消息为 H.323 协议网守拒绝消息，所述注册消息为 H.323 协议注册请求消息，所述注册成功响应消息为 H.323 协议注册成功消息。



密钥分发方法

技术领域

本发明涉及通信中的安全管理技术，尤指一种应用于NGN（下一代网络）中的密钥分发方法。

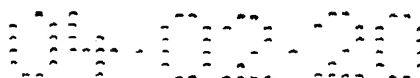
背景技术

NGN是可以提供包括话音、数据和多媒体等各种业务在内的综合开放的网络构架，为用户提供实时的会话业务。其网络设备包括少量的核心设备和大量的用户终端，网络中除了与PSTN/PLMN（公众电信网/公众陆地移动网）的交互是基于电路方式而比较安全外，其它网络设备之间的交互，都是基于分组核心网络及各种分组接入网络来传送。在开放的IP网络上，NGN网络极易受到各种非法的攻击，特别是NGN网络中存在的大量的分组终端，很容易成为非法攻击的发起者。

针对 NGN 网络安全，目前还没有较好的解决方案，而作为网络安全基础的密钥分发过程如何和 NGN 网络的特点结合起来，还是一个空白。现有技术中网络层安全标准 IPSec（网络层安全）定义的密钥协商方式是 IKE 协议（因特网密钥交换协议）、传输层安全标准 TLS（传输层安全）的密钥协商方式是由 TLS 规范定义的 Handshake（握手协议）来完成，其中 IKE 协议的密钥加密交换采用 Diffie-Hellman 算法，定义了 5 个 D-H 算法的参数组（即素数 p 和底数 g ），该加密算法具有强度高、密钥长度大的特点。从上可知，IKE 是一个非常严谨、同时也是一个相当复杂的密钥交换协议，而 Handshake 协议实现客户和服务端之间的一方（主要对服务器）或双向认证，协商协议中用到的加密算法和密钥以及验证算法和密钥，协商得到的会话参数供记录协议为多个连接重复使用，避免每个连接协商新的会话参数所带来的开销，同时协议保证协商过程是可靠的、协商得到的共享密钥是安全的。

尽管上述这些密钥分发协议都很规范、严谨，但都存在无法和 NGN 网络的实际特点相结合的缺点。NGN 网络是一个较为封闭的网络，由一系列网络





侧服务器（如软交换、应用服务器和各种网关）以及大量的接入终端组成，终端和网络设备在一个运营商的管辖和控制范围内，存在一个管理域对域内设备进行管理，以及协助完成跨域之间用户互通的特点，同时所有的终端需要在该管理域内进行注册，NGN 的这些网络特点决定了 NGN 适合于采用集中式的密钥分发方式，而上述密钥分发协议都是终端之间或两台主机直接进行密钥的协商，最终导致系统中的通信量成几何数的增长，给整个网络系统和密钥的管理都带来了很大的不便，不适应 NGN 网络的实际特点。

发明内容

本发明解决的技术问题是提供一种安全、高效的密钥分发方法，可实现集中密钥分发，适应 NGN 的网络特点。

为解决上述问题，本发明提供一种密钥分发方法，包括如下步骤：

- a) 终端向软交换发送注册请求消息；
- b) 软交换向认证中心发送认证请求消息；
- c) 认证中心对终端进行认证，同时生成所述终端与软交换的会话密钥，并在注册认证通过后，交由软交换向终端分发所述会话密钥。

其中，所述步骤 c) 具体包括：

c1) 认证中心根据与终端的共享密钥 Kc 生成对终端的第一验证字，同时生成所述终端与软交换之间的会话密钥，然后以所述共享密钥 Kc 对所述会话密钥加密，将加密后的会话密钥和第一验证字返回给软交换；

c2) 软交换向终端返回注册失败响应消息；

c3) 终端根据与认证中心的共享密钥 Kc 生成第二验证字，然后向软交换发送包含所述第二验证字的注册消息；

c4) 软交换根据认证中心提供的第一验证字与终端提供的第二验证字对所述终端进行认证，并在认证通过后，执行步骤 c5)；

c5) 软交换向终端返回注册成功响应消息，所述注册成功响应消息中包含经共享密钥 Kc 加密后的会话密钥，同时软交换向认证中心发出终端认证成功消息以便更新终端的相关信息；

c6) 终端根据所述共享密钥 Kc 解密认证中心加密过的会话密钥。



进一步, 步骤 c3) 所述注册消息还包含终端支持的安全能力列表及每种安全能力的优先级信息;

步骤 c4) 还包括软交换根据注册消息中终端的安全能力及每种安全能力的优先级信息选择一个合适的安全能力进行通信。

最好, 所述下一代网络还包括信令代理, 所述步骤 a) 具体包括:

终端向信令代理发送注册请求消息, 信令代理向软交换转发终端的注册请求消息;

所述步骤 c1) 进一步包括:

认证中心获取与信令代理的共享密钥 K_{sp} , 然后以所述共享密钥 K_{sp} 对会话密钥进行加密, 并将经共享密钥 K_{sp} 加密后的会话密钥也返回给软交换;

所述步骤 c2) 具体包括:

软交换向信令代理返回注册失败响应消息, 信令代理向终端返回注册失败响应消息, 同时要求终端反馈支持的安全能力列表及每种安全能力的优先级信息;

所述步骤 c3) 具体包括:

终端将包含第二验证字、终端支持的安全能力列表以及每种安全能力的优先级信息的注册消息发送给信令代理, 信令代理根据终端支持的安全能力和每种安全能力的优先级信息选择一个合适的安全能力进行通信, 然后向软交换转发终端的注册消息;

所述步骤 c5) 具体包括:

软交换向信令代理转发终端注册成功响应消息, 所述注册成功响应消息中包含认证中心分别以共享密钥 K_c 和 K_{sp} 加密后的会话密钥, 信令代理用共享密钥 K_{sp} 解密认证中心经共享密钥 K_{sp} 加密过的会话密钥, 并以所述解密获取的会话密钥对注册成功响应消息报文计算报文验证字, 然后信令代理向终端转发注册成功响应消息, 所述注册成功响应消息中包含经共享密钥 K_{sp} 加密过的会话密钥、信令代理根据终端支持的安全能力选定的后续通信采用的安全能力项以及终端的安全能力参数列表和优先级信息以及所述报文验证字;

所述步骤 c6) 进一步包括:

终端利用解密后获取的会话密钥, 验证信令代理返回报文的报文验证字



以验证信令代理身份，同时验证报文的完整性以及信令代理返回的终端自己的安全能力参数是否正确，并在验证通过后，按照选定的安全能力进行通信。

最好，所述注册请求消息和注册消息均为 SIP 协议注册消息，所述注册失败响应消息为 SIP 协议响应消息，所述注册成功响应消息为 SIP 协议注册请求成功消息。

最好，所述注册请求消息为 MGCP 协议系统重启消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 MGCP 协议通知请求消息及其响应消息，所述注册消息为 MGCP 协议通知消息及其响应消息。

最好，所述注册请求消息为 H.248 协议系统服务状态变化消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 H.248 协议属性更改消息及其响应消息，所述注册消息为 H.248 协议通知消息及其响应消息。

最好，所述注册请求消息为 H.323 协议网守请求消息，所述注册失败响应消息为 H.323 协议网守拒绝消息，所述注册消息为 H.323 协议注册请求消息，所述注册成功响应消息为 H.323 协议注册成功消息。

与现有技术相比，本发明具有以下优点：

1、本发明中由软交换与终端通信，在注册认证过程中实现密钥的分发，通信量小，能紧密的结合NGN网络的特点、同时又大大提高了整个系统解决安全问题的效率，终端的注册认证与密钥的集中分发更适合于NGN网络的实际情况。

2、本发明中可实现将SIP、MGCP、H.248、H.323等多个协议注册过程与会话密钥分发过程结合起来，在终端认证过程中完成会话密钥分发，后续的通信不需要再协商密钥。

3、本发明中还可实现将SIP、MGCP、H.248、H.323等多个协议注册过程与安全能力协商过程结合起来，在密钥分发的过程中同时完成安全能力协商，后续的通信不需要再协商安全能力，安全能力不需要进行静态配置，可动态协商，灵活扩展。

附图说明

图 1 是本发明密钥分发方法应用的一种 NGN 网络环境示意图；





图 2 是在图 1 所示的网络环境下本发明密钥分发方法具体实施例通信过程示意图;

图 3 是本发明密钥分发方法应用的具有信令代理的一种 NGN 网络环境示意图;

图 4 是在图 3 所示的网络环境下本发明密钥分发方法具体实施例通信过程示意图;

图 5 是在 SIP 协议注册认证过程中实现密钥分发的实施例通信过程示意图;

图 6 是在 MGCP 协议注册认证过程中实现密钥分发的实施例通信过程示意图;

图 7 是在 H.248 协议注册认证过程中实现密钥分发的实施例通信过程示意图;

图 8 是在 H.323 协议注册认证过程中实现密钥分发的实施例通信过程示意图。

具体实施方式

在 NGN 网络中,网络安全是目前 NGN 网络实际运营中碰到的一个重要问题,如果不能很好的解决 NGN 网络的安全问题,NGN 网络将无法得到大规模的应用。

在 NGN 网络中,网络设备主要包括终端、网关及软交换等,图 1 是 NGN 一种简单的单域组网图,即只有一个软交换(也称为媒体网关控制器)设备,实际组网可能有多个软交换设备。如图 1 所示的 NGN 网络环境中,软交换通过 IP 网络分别与中继媒体网关、SIP(会话初始协议)终端,H.323 终端和 H.248 终端相连,其中中继媒体网关接模拟电话 T1、T2,另外软交换还与认证中心 AuC 相连。

本发明中所有网络设备、终端和认证中心 AuC 之间各有一个共享密钥,网络设备可以采用手工配置或网管下发,终端设备在设备开户时由系统分配或用户输入;





所有与认证中心 AuC 共享密钥为整个系统的基本密钥，需要得到妥善的保管，要求网络设备及终端具有不向第三方泄漏此密钥，以及具有抗非法盗取此密钥的能力；

另外，终端和软交换之间的会话密钥则由认证中心 AuC 生成。

本发明结合 NGN 网络的特点，通过将注册认证过程与会话密钥分发过程结合起来，在终端向软交换发起注册，软交换向认证中心请求认证后，认证中心生成终端与软交换的会话密钥，并在注册认证通过后，由软交换向终端分发会话密钥。由于在注册认证过程中完成会话密钥分发，后续的通信不需要再协商密钥，可使终端的注册认证和密钥的分发过程更简捷，提高了系统的效率和性能，对终端的要求较低，终端不需要支持复杂的密钥分发协议，而只需在现有的呼叫协议上扩展即可。

图 2 是一种简单的密钥分发通信过程示意图，说明如下：

终端首先向软交换发起注册请求，具体消息报文与终端支持的协议相关，软交换收到所述注册请求消息后，向认证中心请求对终端进行认证，认证中心根据终端信息生成相应验证字（便于区别以后称为第一验证字）以及会话密钥，然后向软交换返回认证响应消息，所述认证响应消息中包含所述第一验证字及会话密钥，软交换在收到所述认证响应消息后，向终端发送注册失败响应消息，要求终端重新注册，终端生成验证字（便于区别以后称为第二验证字），然后向软交换重新发起注册请求，软交换比较认证中心与终端提交的第一验证字和第二验证字，若不相同，则向终端返回注册失败响应消息，要求终端重新注册，若相同，则认证通过，向终端发送注册成功响应消息，所述注册成功响应消息中包含会话密钥，终端在收到所述消息后即可获取会话密钥。

为了进一步提高网络的安全性，在软交换向终端返回注册失败响应消息时，软交换还要求终端反馈支持的安全能力列表，这样，终端重新向软交换发起注册时，在注册消息报文中进一步包括终端支持的安全能力列表以及每种安全能力的优先级信息等，软交换可据此选择合适的安全能力进行通信。

事实上为了通信的安全，本发明应用的网络环境中还可包括信令代理（SP），整个网络环境中，信令代理以上的网络设备之间的通信是可信的，即



需要在组网上保证这些网络设备是处于一个信任区内，终端是不可信的，终端和信令代理之间的通信是不安全的，即终端和信令代理位于非信任区，信令代理为信任区和非信任区的边界。

信令代理可以作为一个功能模块与处理媒体转发的模块一起集成在 IP 网关中，也可以采用信令与媒体分离的架构方式，独立出来成为一个单独的信令代理实体，下面以具体实施例进行说明。

图 3 是一种信令代理集成在 IP 网关的网络环境，在所述的网络环境中，终端通过信令代理实现与软交换通信，上述终端与软交换的会话密钥在所述的网络环境中也即终端与信令代理的会话密钥。

图 4 是图 3 所示具信令代理的网络环境中实现密钥分发的通信过程，说明如下。

在步骤 s1.终端按协议流程向信令代理发送注册请求消息，正常的协议注册消息，具体消息报文与终端支持的协议相关，为一个普通的协议注册报文，报文未经加密认证处理，所述注册请求消息报文中包含如下信息：

$IDc \parallel IDsp \parallel N1 \parallel TS1$

- IDc: 标识终端
- IDsp: 标识信令代理
- N1: 随机数或序列号，用于标识本次报文，返回的响应报文中需包含此数，用于防止报文重发（后续消息中的此数含义相同）
- TS1: 用于信令代理验证终端的时钟与信令代理的时钟是否同步；

在步骤 s2.信令代理向软交换转发终端的注册请求消息，该消息报文中包含如下信息：

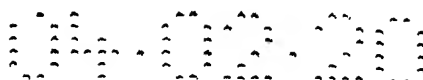
$IDc \parallel IDsp$

- IDc: 标识终端
- IDsp: 标识信令代理；

在步骤 s3.软交换没有终端的鉴权信息，向认证中心（AuC）发出对终端的鉴权认证请求消息，提供终端标识 ID 和信令代理标识 ID，该消息报文中包含信息如下：

$IDc \parallel IDsp$





- IDc: 标识终端;
- IDsp: 标识终端接入网络的信令代理;

在步骤 s4.认证中心根据终端标识 ID、信令代理标识 ID, 获取与终端的共享密钥 Kc 以及与信令代理的共享密钥 Ksp 及其它认证信息, 生成一个挑战字随机数 Rand, 由 Rand, IDc 和共享密钥 Kc 等一起生成对终端的第一验证字 Authenticatorc, 同时生成终端和信令代理之间的会话密钥 Kc,sp, 并分别由共享密钥 Kc 和 Ksp 对所述会话密钥 Kc,sp 加密, 将 Rand、验证字、加密后的会话密钥 Kc,sp 作为软交换认证请求的响应返回给软交换, 该认证响应消息报文中包含如下信息:

IDc || IDsp || Rand || Authenticatorc || EKc [Kc,sp] || EKsp [Kc,sp]

其中: Authenticatorc = f m(Kc, Rand, IDc)

- IDc: 标识终端
- IDsp: 标识信令代理
- Rand: 随机数, 用于认证中心计算验证字, 认证中心将 Rand 发给软交换, 软交换再发给信令代理, 再由信令代理发给终端
- Authenticatorc: 验证字, 用于软交换验证终端, 认证中心生成后发给软交换
- EKc [Kc,sp]: 认证中心以共享密钥 Kc 加密过的会话密钥 Kc,sp
- EKsp [Kc,sp]: 认证中心以共享密钥 Ksp 加密过的会话密钥 Kc,sp

在步骤 5.软交换向信令代理返回注册失败响应消息, 注册失败, 需要对终端进行认证, 注册失败响应消息报文参数中包括挑战字 Rand, 该消息报文中包含如下信息:

IDc || IDsp || Rand

- IDc: 标识终端
- IDsp: 标识信令代理
- Rand: 为认证中心发给信令代理的随机数;

在步骤 6.信令代理向终端返回注册失败响应消息, 注册失败, 需要对终端进行认证, 同样注册失败响应消息报文中包括挑战字 Rand, 同时要求终端反馈支持的安全能力列表和每种安全能力的优先级信息, 该报文中包含如下信息:



$IDc \parallel IDsp \parallel N1 \parallel N2 \parallel TS2 \parallel Rand$

- IDc: 标识终端
- IDsp: 标识信令代理
- N1: 同终端发给信令代理的注册消息报文中的 N1, 用于对注册报文的回应
- N2: 用于标识本次报文
- TS2: 用于终端验证时间戳
- Rand: 为认证中心生成的随机数;

在步骤 7.终端通过共享密钥 Kc、客户段标识 IDc 及信令代理返回的随机数 Rand 重新计算验证字, 向信令代理重新发起注册, 注册消息报文中包括新计算得到的第二验证字 Authenticatorc, 同时注册消息报文中包含终端支持的安全能力列表 (如网络层安全 IPSec、传输层安全 TLS 或应用层安全等), 以及每一种安全能力的优先级信息, 信令代理将根据终端的安全能力和优先级信息选择一个合适的安全能力进行通信, 该注册消息报文中包含如下信息:

$IDc \parallel N1 \parallel N2 \parallel TS3 \parallel Authenticatorc \parallel Security\ mechanism\ list$

其中: $Authenticatorc = f(Kc, Rand, IDc)$

- IDc: 标识终端;
- N1: 新的随机数或序列号, 用于标识本次报文
- N2: 用于标识对信令代理上一个报文的回应
- TS3: 让信令代理验证时间戳
- Authenticatorc: 验证字, 由终端生成
- Security mechanism list: 终端的安全能力及优先级列表;

在步骤 8.信令代理向软交换转发终端的注册消息报文, 对于终端的安全能力和优先级信息参数可以转发, 也可以不转发, 软交换不需该信息, 该注册消息报文中包含如下信息:

$IDc \parallel IDsp \parallel Authenticatorc$

- IDc: 标识终端
- IDsp: 标识信令代理
- Authenticatorc: 验证字, 由终端生成;

在步骤 9.软交换将信令代理发过来的注册消息报文中的第二验证字和认



证中心发过来的第一验证字进行比较,对终端进行验证,若两者不一致,则验证失败,可重发注册失败响应消息,若两者一致,则表明对终端的验证成功,向信令代理返回注册成功响应消息报文,该消息报文中同时包括两个由认证中心生成的分别经过 K_c 和 K_{sp} 加密后的终端与信令代理之间的会话密钥 $K_{c,sp}$,该消息报文中包含如下信息:

$ID_c \parallel ID_{sp} \parallel EK_c[K_{c,sp}] \parallel EK_{sp}[K_{c,sp}]$

- ID_c : 标识终端
- ID_{sp} : 标识信令代理
- $EK_c[K_{c,sp}]$: 为认证中心用共享密钥 K_c 加密的终端与信令代理之间的会话密钥 $K_{c,sp}$
- $EK_{sp}[K_{c,sp}]$: 为认证中心用共享密钥 K_{sp} 加密的终端与信令代理之间的会话密钥 $K_{c,sp}$;

在步骤 10.信令代理收到软交换的注册响应成功消息,向终端转发注册成功响应消息,该消息报文中包含由认证中心生成的经过终端的共享密钥 K_c 加密后的会话密钥 $K_{c,sp}$,同时注册成功响应消息中包括信令代理依据终端的安全能力参数选定的后续通信采用的安全能力项以及终端的安全能力参数列表和优先级信息(用于终端确认这些参数是否在网络传输中被第三者修改),最后用共享密钥 K_{sp} 对由认证中心生成的经过 K_{sp} 加密后的会话密钥 $K_{c,sp}$ 进行解密处理,得到 $K_{c,sp}$,并用 $K_{c,sp}$ 对整个响应消息报文计算报文验证字 MAC,用于保证报文的完整性,以及终端对信令代理的认证,报文中包含如下信息:

$ID_c \parallel ID_{sp} \parallel N1 \parallel N2 \parallel TS4 \parallel EK_c[K_{c,sp}] \parallel \parallel \text{Security mechanism} \parallel \text{Security mechanism list}(c) \parallel fm(K_{c,sp}, \text{报文})$

- ID_c : 标识终端
- ID_{sp} : 标识信令代理
- $N1$: 用于标识对终端注册报文的回应
- $N2$: 用于标识本次报文
- $TS4$: 用于终端验证时间戳
- $EK_c[K_{c,sp}]$: 为认证中心用共享密钥 K_c 加密的终端与信令代理之间的会话密钥 $K_{c,sp}$



- Security mechanism: 信令代理根据终端的安全能力及优先级列表选定的安全能力
- Security mechanism list: 终端自己的安全能力及优先级列表, 用于终端确认信令代理收到的安全能力列表没有被非法修改过
- fm(Kc,sp, 报文): 用会话密钥 Kc,sp 对整个报文进行源和完整性认证, 终端通过解开会话密钥, 并对报文进行成功鉴别来实现对信令代理的身份认证, 否则信令代理无法得到由认证中心签发的会话密钥 Kc,sp;

在步骤 11. 软交换向认证中心发出终端认证成功消息, 更新终端的相关信息, 同时终端对由认证中心生成的经过 Ksp 加密后的会话密钥解密得到 Kc,sp, 并用 Kc,sp 验证信令代理返回报文的 MAC, 实现对信令代理的身份验证, 同时验证报文的完整性, 以及信令代理返回的终端自身的安全能力参数是否正确, 如果正确, 则说明信令代理返回的选定的安全能力正确, 后续通信将按此安全能力进行报文安全处理, 如果终端对信令代理认证失败或安全能力参数不正确, 可重新发起注册, 该终端认证成功消息报文中包含如下信息:

IDc || IDsp || IPc || ...

- IDc: 标识终端
- IDsp: 标识信令代理

IPc: 终端注册的 IP 地址, 可能是经过信令代理变换处理后的 IP 地址。

下面以具体的应用协议环境对本发明密钥分发方法进行说明。

图 5 是本发明采用 SIP 协议进行注册认证的具体通信过程, 仍以网络环境为具有信令代理为例, 所述通信过程中只是将上述通用流程中的注册和响应消息细化为具体的 SIP 协议消息, 流程中每一步骤的消息所携带的参数与上述通用流程中的定义是一致的。

所述通信过程中具体的协议消息, 在步骤 s1、步骤 s2, 注册请求消息为 SIP 协议中的注册消息; 在步骤 s5、步骤 s6, 注册失败响应消息为 SIP 协议中的响应消息代码, 其中 401: 为 SIP 协议中的响应消息代码, 含义为需要对终端进行认证, 407: 为 SIP 协议中的响应消息代码, 含义为需要对代理进行



认证, 在步骤 s7、步骤 s8, 重新注册消息也为 SIP 协议中的注册消息; 在步骤 s9、步骤 s10, 注册成功响应消息为 SIP 协议中的响应消息代码, 表示请求成功, 即 OK; 而步骤 s3、s4、s11 中的消息, 则与具体的呼叫协议没有关系, 可以是通用的认证协议, 根据应用场合的不同, 可以采取不同的协议, 如 Radius、Diameter 等。

图 6 是本发明采用 MGCP (媒体网关控制协议) 协议进行注册认证的具体通信过程, 仍以网络环境为具有信令代理为例, 所述通信过程中只是将上述通用流程中的注册和响应消息细化为具体的 MGCP 协议消息, 流程中每一步骤的消息所携带的参数与上述通用流程中的定义是一致的。

所述通信过程中具体的协议消息, 在步骤 s1、步骤 s2, 注册请求消息为 MGCP 协议中的系统重起消息命令 RSIP 及其响应消息; 在步骤 s5、步骤 s6, 注册失败响应消息为 MGCP 协议中的通知请求消息命令 RQNT, 表示系统需要对终端进行认证, 在步骤 s7、步骤 s8, 重新注册消息为 MGCP 协议中的通知消息命令 NOTIFY, 表示终端发起认证; 在步骤 s9、步骤 s10, 注册成功响应消息为 MGCP 协议中的通知请求消息命令 RQNT, 通知终端认证成功; 而步骤 s3、s4、s11 中的消息, 则与具体的呼叫协议没有关系, 可以是通用的认证协议, 根据应用场合的不同, 可以采取不同的协议, 如 Radius、Diameter 等。

图 7 是本发明采用 H.248 协议进行注册认证的具体通信过程, 仍以网络环境为具有信令代理为例, 所述通信过程中只是将上述通用流程中的注册和响应消息细化为具体的 H.248 协议消息, 流程中每一步骤的消息所携带的参数与上述通用流程中的定义是一致的。

所述通信过程中具体的协议消息, 在步骤 s1、步骤 s2, 注册请求消息为 H.248 协议中的系统服务状态变化消息命令 SERVICE CHANGE 及其响应消息 Rsp, 此时表明系统开始进入服务状态, 发起注册; 在步骤 s5、步骤 s6, 注册失败响应消息为 H.248 协议中的属性更改消息命令 MODIFY, 表示系统需要对终端进行认证, 在步骤 s7、步骤 s8, 重新注册消息为 H.248 协议中的通知消息命令 NOTIFY, 表示终端发起认证; 在步骤 s9、步骤 s10, 注册成功响应消息为 H.248 协议中的属性更改消息命令 MODIFY, 通知终端认证成功; 而步骤 s3、s4、s11 中的消息, 则与具体的呼叫协议没有关系, 可以是通用的认



证协议, 根据应用场合的不同, 可以采取不同的协议, 如 Radius、Diameter 等。

图 8 是本发明采用 H.323 协议进行注册认证的具体通信过程, 仍以网络环境为具有信令代理为例, 所述通信过程中只是将上述通用流程中的注册和响应消息细化为具体的 H.323 协议消息, 流程中每一步骤的消息所携带的参数与上述通用流程中的定义是一致的。

所述通信过程中具体的协议消息, 在步骤 s1、步骤 s2, 注册请求消息为 H.323 协议中的 GK 请求消息, 含义为谁是我的 GK; 在步骤 s5、步骤 s6, 注册失败响应消息为 H.323 协议中的 GK 拒绝消息, 含义为 GK 不对终端进行注册, 此处表示需要认证, 在步骤 s7、步骤 s8, 重新注册消息为 H.323 协议中的注册请求消息, 此时消息中将携带认证信息, 表示终端发起认证; 在步骤 s9、步骤 s10, 注册成功响应消息为 H.323 协议中的注册成功消息, 通知终端认证成功; 而步骤 s3、s4、s11 中的消息, 则与具体的呼叫协议没有关系, 可以是通用的认证协议, 根据应用场合的不同, 可以采取不同的协议, 如 Radius、Diameter 等。

综上本发明具有下面的优点:

在一个流程中实现了终端的注册、认证, 用户终端设备和网络设备之间的密钥分发和安全能力协商; 交互流程简洁高效;

交互流程及认证机制能保证终端注册、会话密钥分发, 安全能力协商过程本身也是安全的;

同时本发明通过将多个流程有机的融合为一体, 避免了后续还要进行密钥分发和安全能力的配置等, 提高了整个 NGN 网络系统在安全方面的处理效率。

以上所述, 仅为本发明的优选实施例而已, 非因此即局限本发明的权利范围, 凡运用本发明说明书及附图内容所为的等效变化, 均理同包含于本发明的权利要求范围内。



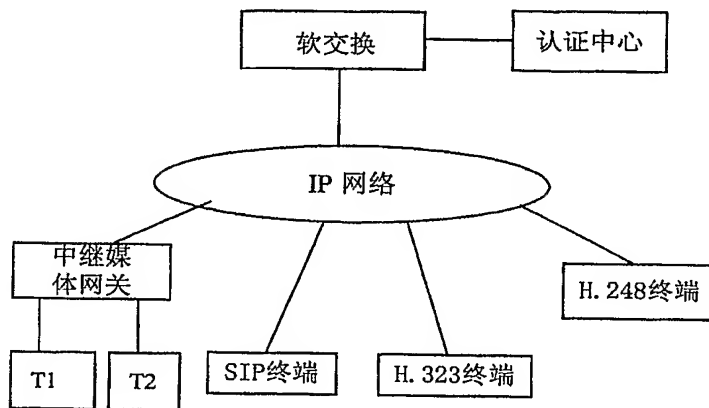


图 1

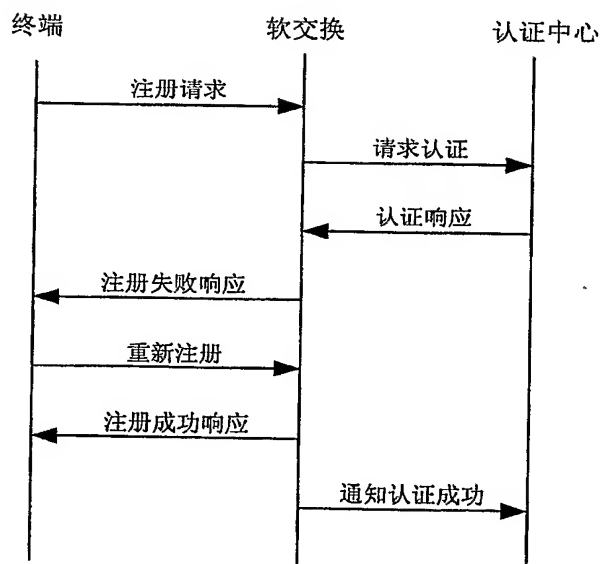


图 2



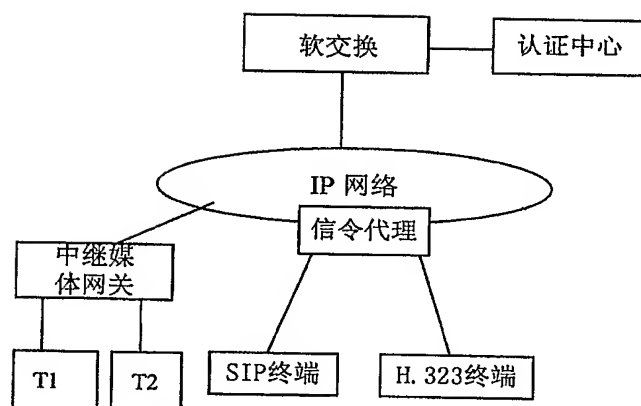


图 3



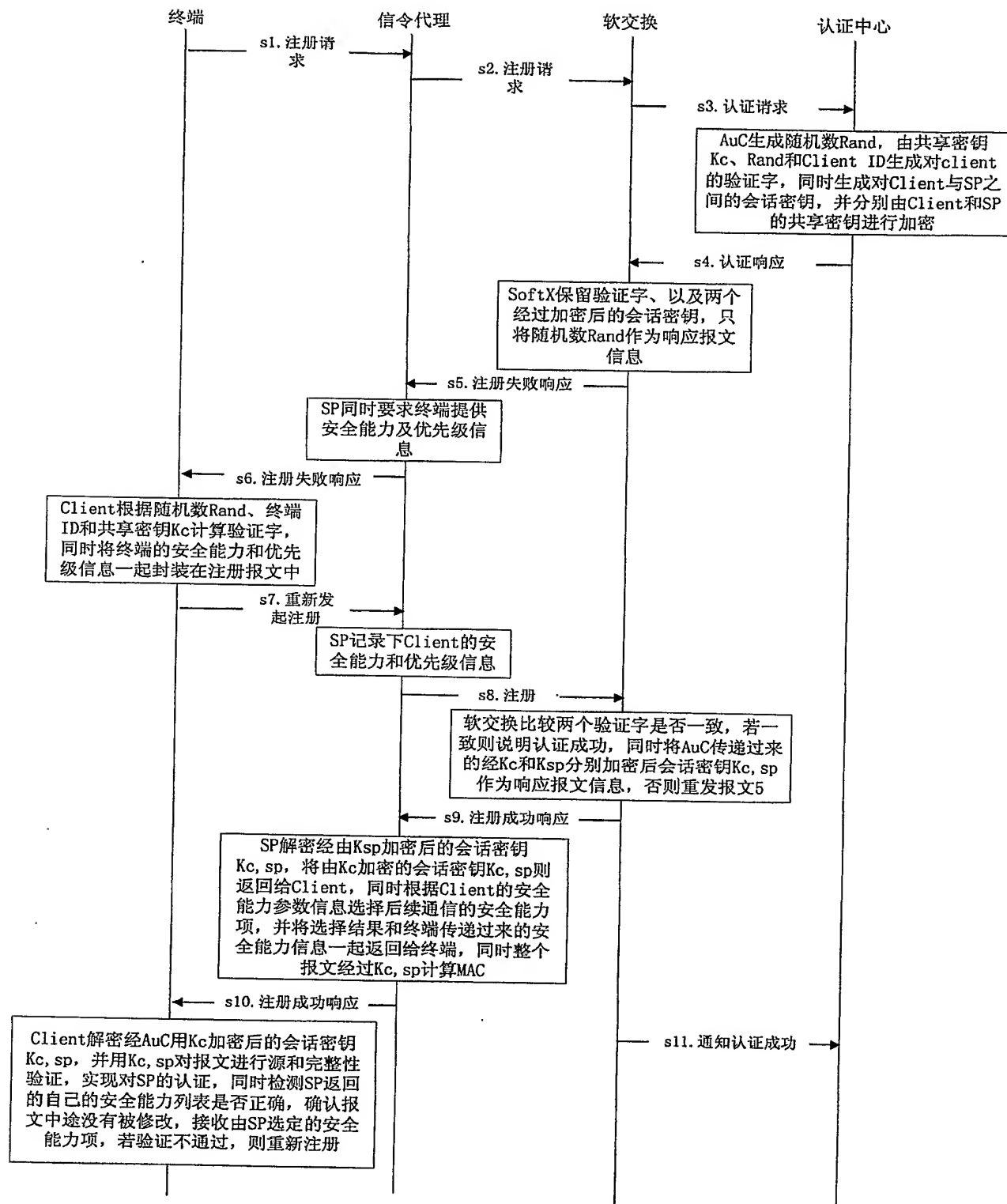


图 4



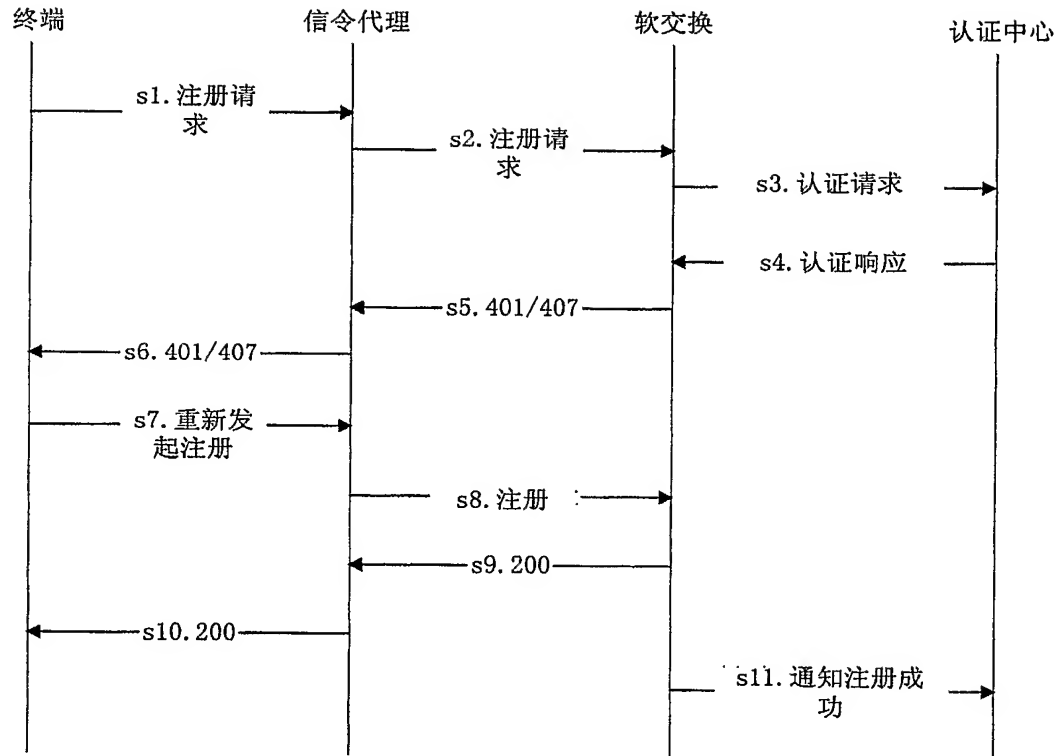


图 5



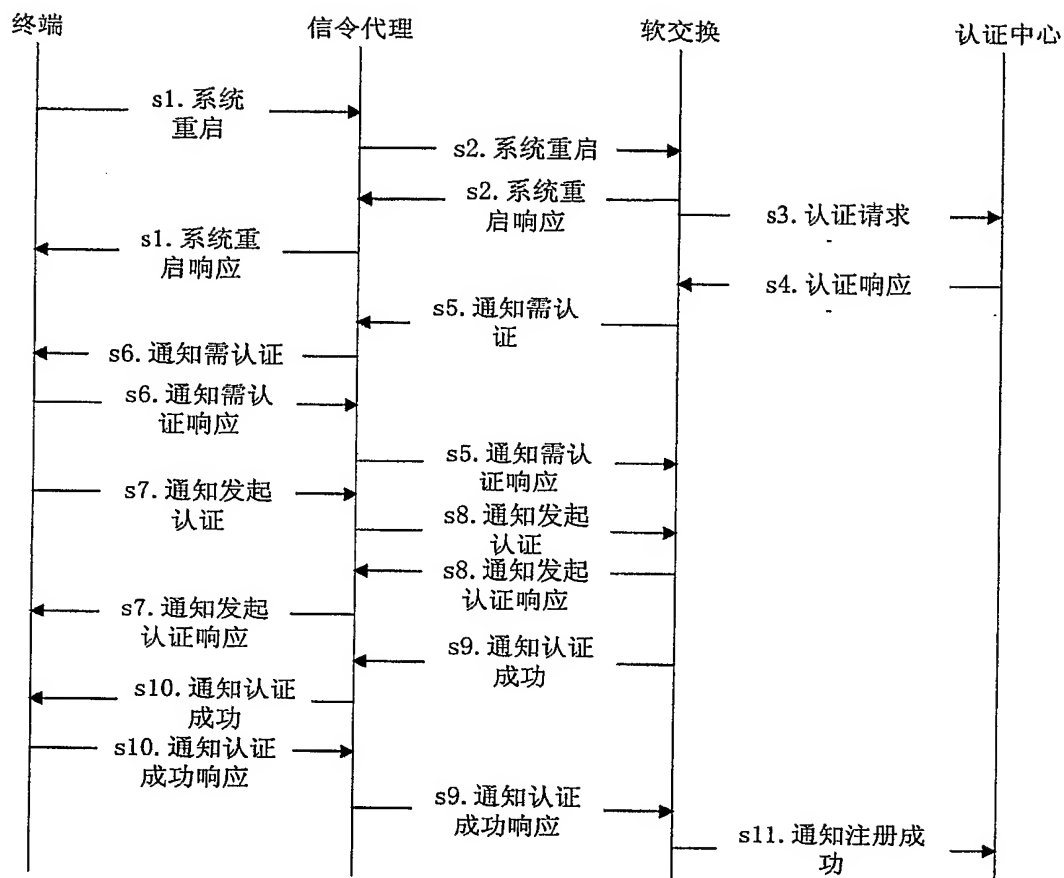


图 6



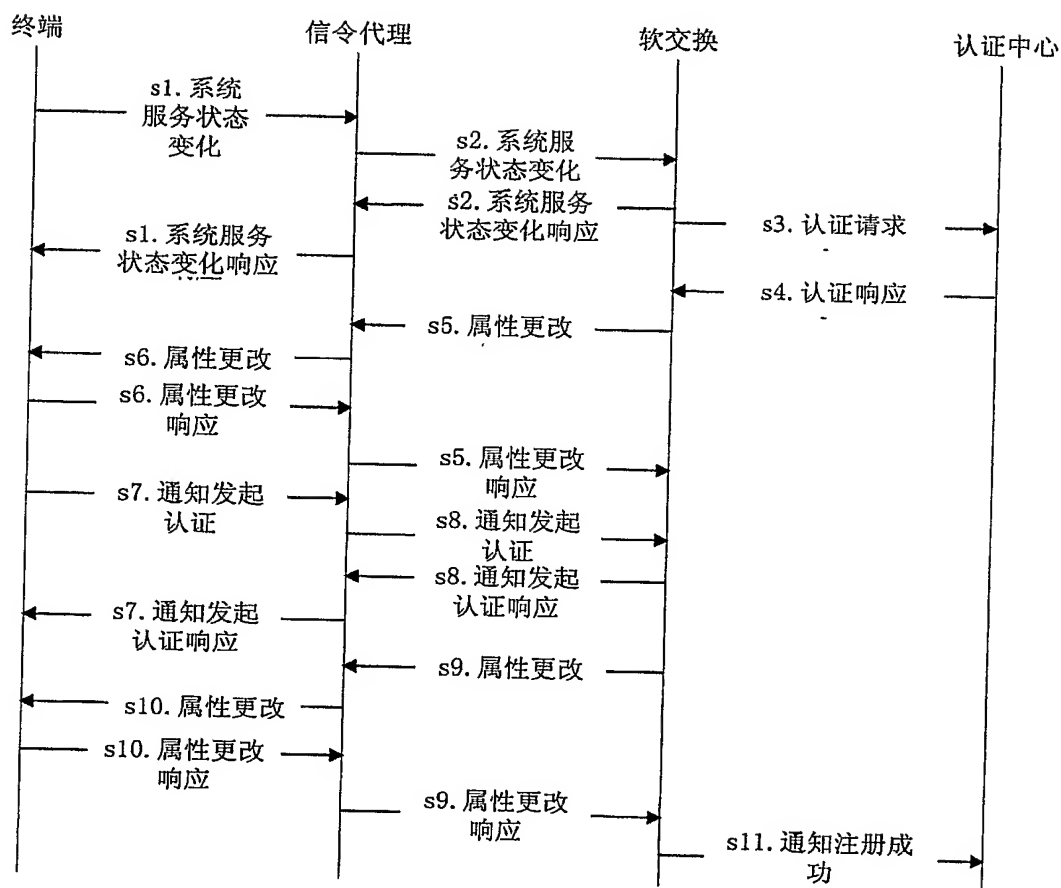


图 7



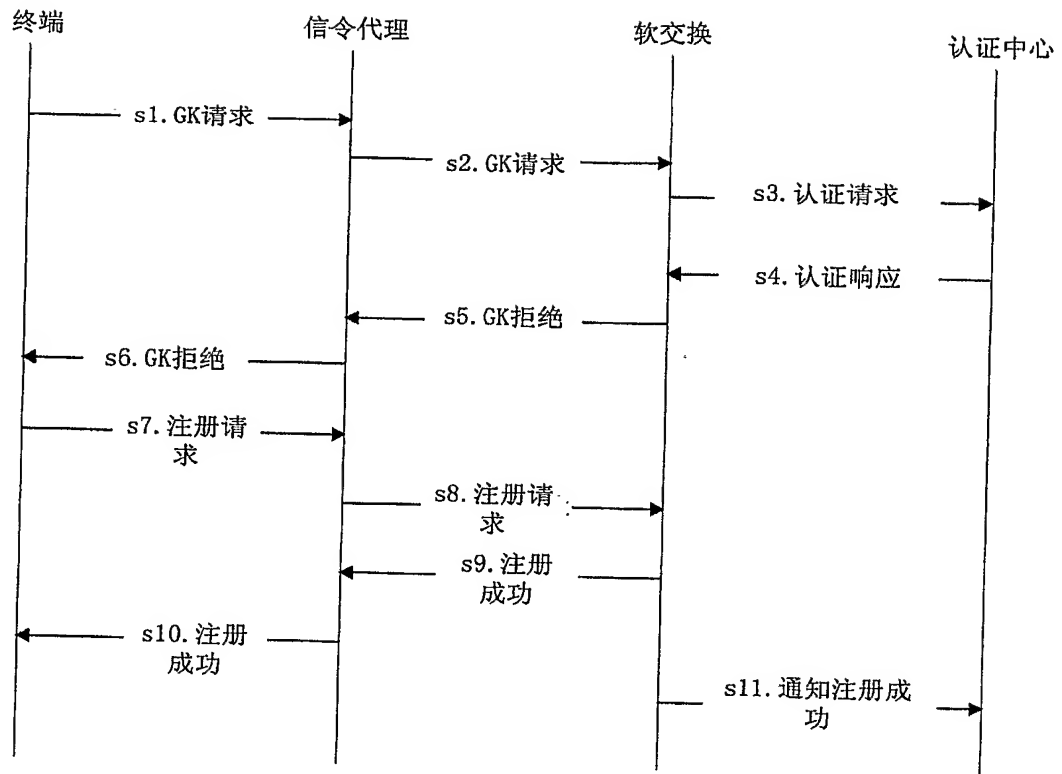


图 8

